Finite Fields and Their Applications 15 (2009) 23–39

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On the distinctness of maximal length sequences over $Z/(pq)$ modulo 2 ☆

Hua-Jin Chen, Wen-Feng Qi *

Zhengzhou Information Science and Technology Institute, PO Box 1001-745, Zhengzhou 450002, People's Republic of China

ARTICLE INFO

Article history:
Received 24 April 2008
Revised 24 July 2008
Available online 13 August 2008
Communicated by Gary L. Mullen

Keywords:
Integer residue ring
Modular reduction
Primitive polynomial
Primitive sequence

ABSTRACT

This paper studies the distinctness problem of the reductions modulo 2 of maximal length sequences over $Z/(pq)$, where p and q are two different odd primes with $p < q$. A polynomial $f(x)$ over $Z/(pq)$ is called primitive if $f(x)$ modulo p and $f(x)$ modulo q are primitive over $Z/(p)$ and $Z/(q)$, respectively. A primitive element in $Z/(pq)$ is defined analogously. Let $\underline{a}$ and $\underline{b}$ be two maximal length sequences generated by a primitive polynomial $f(x)$ over $Z/(pq)$. Firstly, for the case of $\deg f(x) > 1$, it is proved that if there exist a nonnegative integer S and a primitive element ξ in $Z/(pq)$ such that $x^S - \xi \equiv 0 \pmod{f(x), pq}$, and either $(q-1)$ is not divisible by $(p-1)$ or $2(p-1)$ divides $(q-1)$, then $\underline{a} \equiv \underline{b} \pmod 2$ if and only if $\underline{a} = \underline{b}$. The existence of S and ξ is completely determined by p, q and $\deg f(x)$. Secondly, for the case of $\deg f(x) = 1$, it is proved that if $\gcd(p-1, q-1) = 2$ and $(p-1)/\mathrm{ord}_p(2)$ is congruent to $(q-1)/\mathrm{ord}_q(2)$ modulo 2, then $\underline{a} \equiv \underline{b} \pmod 2$ if and only if $\underline{a} = \underline{b}$.

1. Introduction

For an integer $N \geqslant 2$, let $Z/(N)$ be the integer residue ring modulo N, which can be represented as $\{0, 1, \ldots, N-1\}$. In this paper, given an integer a, we always consider $a \pmod N$ to be an element in $\{0, 1, \ldots, N-1\}$.

☆ This work was supported by the NSF of China under Grant number 60673081, the National 863 Plan under Grant numbers 2006AA01Z417 and 2007AA01Z212.

* Corresponding author.
E-mail address: wenfeng.qi@263.net (W.-F. Qi).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2008.07.005

If a sequence $\underline{a} = \{a(i)\}_{i\geqslant 0}$ over $Z/(N)$ satisfies a linear recurrence relation

$$a(i+n) \equiv -\big[c_0 a(i) + c_1 a(i+1) + \cdots + c_{n-1} a(i+n-1)\big] \pmod{N}, \quad i = 0, 1, 2, \ldots$$

with constant coefficients $c_0, c_1, \ldots, c_{n-1} \in Z/(N)$, then $\underline{a}$ is called a *linear recurring sequence* of degree n generated by $f(x)$ over $Z/(N)$, where $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$, and $f(x)$ is called the *characteristic polynomial* of $\underline{a}$. For convenience, denote $G(f(x), N)$ as the set of all linear recurring sequences over $Z/(N)$ generated by $f(x)$.

Let p be a prime and $f(x)$ be a monic polynomial of degree n over $Z/(p^e)$. If $f(0) \neq 0 \pmod{p}$, then there always exists a positive integer P such that $f(x)$ divides $x^P - 1$ over $Z/(p^e)$. The least such P is called the (least) period of $f(x)$ over $Z/(p^e)$ and denoted by $per(f(x), p^e)$. Generally, $per(f(x), p^e) \leqslant p^{e-1}(p^n - 1)$, see [1]. If $per(f(x), p^e) = p^{e-1}(p^n - 1)$, then $f(x)$ is called a *primitive polynomial* of degree n over $Z/(p^e)$. A sequence $\underline{a}$ over $Z/(p^e)$ is called a *primitive sequence* if $\underline{a}$ is generated by a primitive polynomial and $\underline{a} \neq \underline{0} \pmod{p}$. Any element a in $Z/(p^e)$ has a unique p-adic expansion such as $a = a_0 + a_1 \cdot p + \cdots + a_{e-1} \cdot p^{e-1}$, where $a_i \in \{0, 1, \ldots, p-1\}$ for $0 \leqslant i \leqslant e-1$. Similarly, a sequence $\underline{a}$ over $Z/(p^e)$ also has a unique p-adic expansion such as $\underline{a} = \underline{a}_0 + \underline{a}_1 \cdot p + \cdots + \underline{a}_{e-1} \cdot p^{e-1}$, where each $\underline{a}_i$ is a sequence over the prime field $Z/(p)$ and is called the ith-level sequence of $\underline{a}$ for $0 \leqslant i \leqslant e-1$. Often $\underline{a}_{e-1}$ is also called the highest level sequence of $\underline{a}$. Let $f(x)$ be a primitive polynomial over $Z/(p^e)$ and $G'(f(x), p^e)$ denote the set of all primitive sequences generated by $f(x)$ over $Z/(p^e)$. A function $\varphi(x_0, x_1, \ldots, x_{e-1})$ of e variables over $Z/(p)$ is called injective if the induced map $\varphi : G'(f(x), p^e) \to (Z/(p))^\infty$, $\underline{a} \mapsto \varphi(\underline{a}_0, \underline{a}_1, \ldots, \underline{a}_{e-1})$ is injective. Injective functions are one of the main research subjects on primitive sequences over $Z/(p^e)$.

Early in the 1990s, Huang and Dai in [1] and Kuzmin and Nechaev in [2] independently proved that the function x_{e-1} was injective. In other words, a primitive sequence is uniquely determined by its highest level sequence. This important result implies that the highest level sequence $\underline{a}_{e-1}$ contains all information of the original sequence $\underline{a}$. Later on, more and more general injective functions were found and proved.

As for $p = 2$, it was shown in [3–6] that almost all Boolean functions $\varphi(x_0, x_1, \ldots, x_{e-1})$ with e variables containing x_{e-1} were injective. For an odd prime p, references [7–9] showed that functions over $Z/(p)$ of the form $g(x_{e-1}) + \eta(x_0, x_1, \ldots, x_{e-2})$ were injective too, where $1 \leqslant \deg g \leqslant p-1$ and $\eta \in Z/(p)[x_0, x_1, \ldots, x_{e-2}]$. On the other hand, the distinctness of highest level sequences was further improved by Zhu in [10,11], which says that the primitive sequence of p^e elements is uniquely determined by the distribution of element 0 in the highest-level sequence.

Feedback with carry shift registers (FCSRs) were introduced by A. Klapper and M. Goresky in [12]. The main characteristic of FCSRs is the fact that the elementary additions are not additions modulo 2 but with propagation of carries. Lots of researches have been done on the structure and properties of FCSRs and sequences generated by them, especially on the maximal length sequences (or l-sequences), see [13–18]. Let q be an odd number and $\underline{a} = \{a(i)\}_{i\geqslant 0}$ be an output sequence of an FCSR with connection integer q. Then there exists an integer $A \in Z/(q)$ such that $A \neq 0$ and $a(i) = A \cdot 2^{-i} \pmod{q \bmod 2}$, $i \geqslant 0$, where the notation "mod q mod 2" means that first the number $A \cdot 2^{-i}$ is reduced modulo q to give a number between 0 and $q-1$, and then that number is reduced modulo 2. This is also called the exponential representation of FCSR sequences, see [19]. If 2 is a primitive root modulo q and A is coprime with q, then by this exponential representation, it is easily seen that $\underline{a}$ is in fact a reduction sequence of a primitive sequence over $Z/(q)$ modulo 2. In this case, it is necessary that q be a power of a prime $q = p^e$.

Considering such relationship between primitive sequences over rings and FCSR sequences, Zhu studied modular reductions of maximal length sequences over $Z/(p^e)$, where p is an odd prime. It was shown in [20] that for any positive integer M which has a prime factor other than p, if $f(x)$ is a primitive polynomial over $Z/(p^e)$, then for $\underline{a}, \underline{b} \in G(f(x), p^e)$, $\underline{a} = \underline{b}$ if and only if $\underline{a} \equiv \underline{b} \pmod{M}$. Since the operation of mod M destroys the linear structure of the original sequence over $Z/(p^e)$, the reduction sequence $\underline{a} \pmod{M}$ is thought to possess many good cryptographical properties.

Following the work of Zhu in [20], we study the distinctness of primitive sequences over $Z/(pq)$ modulo 2 (the definition of primitive sequences over $Z/(pq)$ refers to Section 2), where p and q are two different odd primes. Our main results proved in this paper are

Theorem 1. *Let p and q be two different odd primes with $p < q$ and $f(x)$ be a primitive polynomial of degree $n > 1$ over $Z/(pq)$. If*

(i) *there exist a nonnegative integer S and a primitive element ξ in $Z/(pq)$ such that $x^S - \xi \equiv 0 \pmod{f(x), pq}$;*
(ii) *$(q-1)$ is not divisible by $(p-1)$ or $2(p-1)$ divides $(q-1)$,*

then $\underline{a} \equiv \underline{b} \pmod 2$ if and only if $\underline{a} = \underline{b}$ for $\underline{a}, \underline{b} \in G'(f(x), pq)$.

Theorem 2. *Let p and q be two different odd primes with $\gcd(p-1, q-1) = 2$ and $f(x)$ be a primitive polynomial over $Z/(pq)$ of degree 1. If $2^{(p-1)/2} \equiv 1 \pmod p$ if and only if $2^{(q-1)/2} \equiv 1 \pmod q$, then $\underline{a} \equiv \underline{b} \pmod 2$ if and only if $\underline{a} = \underline{b}$ for $\underline{a}, \underline{b} \in G'(f(x), pq)$.*

The paper is organized as follows. Section 2 presents some necessary preliminaries. Section 3 is largely devoted to the proofs of our main results. Conclusions are drawn in Section 4.

2. Preliminaries

Let p and q be fixed two different odd primes in this section.

For a periodic sequence $\underline{a} = \{a(i)\}_{i \geqslant 0}$ and a positive integer M, let $per(\underline{a}, M)$ denote the (least) period of $\underline{a} \pmod M$ over $Z/(M)$, which is defined by the least positive integer P such that $a(t+P) \equiv a(t) \pmod M$ for all integer $t \geqslant 0$. Let $N_M(\underline{a}, x)$ denote the number of element x occurring in a complete period of sequence $\underline{a} \pmod M$.

A polynomial $f(x)$ of degree n over $Z/(pq)$ is called primitive if $f(x)$ modulo p and $f(x)$ modulo q are primitive over $Z/(p)$ and $Z/(q)$, respectively. Consequently, a sequence $\underline{a}$ in $G(f(x), pq)$ is called a *primitive sequence* if $\underline{a} \neq \underline{0} \pmod p$ and $\underline{a} \neq \underline{0} \pmod q$. Then in this case we have $per(\underline{a}, pq) = \operatorname{lcm}(p^n - 1, q^n - 1)$. Let $G'(f(x), pq)$ denote the set of all primitive sequences in $G(f(x), pq)$.

Remark 2.1. Note that a primitive sequence over $Z/(pq)$ is always a maximal length sequence, but the converse is not true.

For convenience, for an integer x and positive integer M, we denote the nonnegative minimal residue of x modulo M as $[x]_{\bmod M}$, that is, $[x]_{\bmod M} \equiv x \pmod M$ and $[x]_{\bmod M} \in \{0, 1, \ldots, M-1\}$. This notation has the following simple property.

Property 2.1. *Let x be an arbitrary integer. Then*

$$[p \cdot x]_{\bmod pq} = p \cdot [x]_{\bmod q} \quad \text{and} \quad [q \cdot x]_{\bmod pq} = q \cdot [x]_{\bmod p}.$$

Lemma 2.1. *(See [20].) Let $f(x)$ be a primitive polynomial over $Z/(p^e)$ with positive integer e. For any positive integer M which has a prime factor different from p, $\underline{a} \equiv \underline{b} \pmod M$ if and only if $\underline{a} = \underline{b}$ for $\underline{a}, \underline{b} \in G(f(x), p^e)$. In particular, $\underline{a} \equiv \underline{b} \pmod 2$ if and only if $\underline{a} = \underline{b}$ for $\underline{a}, \underline{b} \in G(f(x), p^e)$.*

Lemma 2.2. *(See [19].) Let q be an odd number and $\underline{a} = \{a(i)\}_{i \geqslant 0}$ be an output sequence of an FCSR with connection integer q. Then there exists an integer $A \in Z/(q)$ such that $A \neq 0$ and*

$$a(i) = A \cdot 2^{-i} \pmod{q \bmod 2}, \quad i = 0, 1, 2, \ldots.$$

Furthermore,

$$\sum_{i=0}^{\infty} a_i 2^i = -\frac{A}{q}.$$

3. Main results

3.1. Primitive polynomials of degree greater than 1

In this subsection, let p and q be fixed two different odd primes.

Lemma 3.1. *Let $f(x)$ be a primitive polynomial of degree $n > 1$ over $Z/(pq)$, and $\underline{a} \in G'(f(x), pq)$. If there exist a positive integer S and a primitive element ξ in $Z/(pq)$ such that $x^S - \xi \equiv 0 \pmod{f(x), pq}$, then there exist two positive integers u and v such that $\gcd(u, q) = 1$, $\gcd(v, p) = 1$ and*

$$a(i + j \cdot S) \equiv p \cdot u \cdot \xi^j \cdot a(i) + q \cdot v \cdot \xi^j \cdot a(i) \pmod{pq}$$

for $i, j \geqslant 0$.

Proof. Since $x^S - \xi \equiv 0 \pmod{f(x), pq}$, it follows that

$$x^{S \cdot j} \equiv \xi^j \pmod{f(x), pq}, \quad j \geqslant 0.$$

This implies that

$$L^{S \cdot j}\underline{a} \equiv \xi^j \cdot \underline{a} \pmod{pq}, \quad j \geqslant 0,$$

where L is the left-shift operator of sequences. So we have

$$a(i + j \cdot S) \equiv \xi^j \cdot a(i) \pmod{pq}, \quad i, j \geqslant 0. \tag{1}$$

Note that p and q are two different odd primes, from Euclidean algorithm we know that there exist two integers u and v satisfying

$$pu + qv = 1, \tag{2}$$

where $\gcd(u, q) = 1$ and $\gcd(v, p) = 1$. Hence (1) and (2) yield

$$a(i + j \cdot S) \equiv p \cdot u \cdot \xi^j \cdot a(i) + q \cdot v \cdot \xi^j \cdot a(i) \pmod{pq}, \quad i, j \geqslant 0. \qquad \square$$

Lemma 3.2. *Let $f(x)$ be a primitive polynomial of degree $n > 1$ over $Z/(pq)$ and $\underline{a}, \underline{b} \in G'(f(x), pq)$ such that $\underline{a} \equiv \underline{b} \pmod 2$. If there exist a positive integer S and a primitive element ξ in $Z/(pq)$ such that $x^S - \xi \equiv 0 \pmod{f(x), pq}$, then*

$$\left[a\left(i^*\right)\right]_{\bmod q} = \left[b\left(i^*\right)\right]_{\bmod q}$$

for any nonnegative integer i^* with $[a(i^*)]_{\bmod p} = [b(i^*)]_{\bmod p} = 0$.

Proof. On one hand, since $[a(i^*)]_{\bmod p} = [b(i^*)]_{\bmod p} = 0$, by Lemma 3.1 we have

$$a\left(i^* + j \cdot S\right) \equiv p \cdot u \cdot \xi^j \cdot a\left(i^*\right) \pmod{pq}, \quad j \geqslant 0,$$
$$b\left(i^* + j \cdot S\right) \equiv p \cdot u \cdot \xi^j \cdot b\left(i^*\right) \pmod{pq}, \quad j \geqslant 0.$$

Then Property 2.1 implies that

$$a(i^* + j \cdot S) \equiv p \cdot \left[u \cdot \xi^j \cdot a(i^*)\right]_{\bmod q}, \quad j \geqslant 0, \tag{3}$$

$$b(i^* + j \cdot S) \equiv p \cdot \left[u \cdot \xi^j \cdot b(i^*)\right]_{\bmod q}, \quad j \geqslant 0. \tag{4}$$

On the other hand, we have

$$a(i^* + j \cdot S) \equiv b(i^* + j \cdot S) \pmod 2, \quad j \geqslant 0, \tag{5}$$

by the assumption of $\underline{a} \equiv \underline{b} \pmod 2$. Thus, (3), (4) and (5) yield

$$\left[u \cdot \xi^j \cdot a(i^*)\right]_{\bmod q} \equiv \left[u \cdot \xi^j \cdot b(i^*)\right]_{\bmod q} \pmod 2, \quad j \geqslant 0. \tag{6}$$

Note that both $\{[u \cdot \xi^j \cdot a(i^*)]_{\bmod q}\}_{j \geqslant 0}$ and $\{[u \cdot \xi^j \cdot b(i^*)]_{\bmod q}\}_{j \geqslant 0}$ are sequences generated by the primitive polynomial $x - \xi$ over $Z/(q)$, and so it follows from Lemma 2.1 that

$$u \cdot a(i^*) \equiv u \cdot b(i^*) \pmod q.$$

Then $a(i^*) \equiv b(i^*) \pmod q$ since $\gcd(u, q) = 1$. The lemma is proved. □

In the following, we are going to deal with the case of $[a(i^*)]_{\bmod p} = [b(i^*)]_{\bmod p} \neq 0$ in Lemmas 3.3 and 3.4.

Lemma 3.3. *Let $f(x)$ be a primitive polynomial of degree $n > 1$ over $Z/(pq)$, and $\underline{a}, \underline{b} \in G'(f(x), pq)$ such that $\underline{a} \equiv \underline{b} \pmod 2$. If $p < q$ and the following two conditions are satisfied*:

(i) *there exist a positive integer S and a primitive element ξ in $Z/(pq)$ such that $x^S - \xi \equiv 0 \pmod{f(x), pq}$;*
(ii) *$(q-1)$ is not divisible by $(p-1)$ or $2(p-1)$ divides $(q-1)$,*

then

$$\left[a(i^*)\right]_{\bmod q} = \left[b(i^*)\right]_{\bmod q}$$

for any nonnegative integer i^* with $[a(i^*)]_{\bmod p} = [b(i^*)]_{\bmod p} \neq 0$.

Proof. Assume $[a(i^*)]_{\bmod p} = [b(i^*)]_{\bmod p} = x \neq 0$. It follows from Lemma 3.1 that

$$a(i^* + j \cdot S) \equiv p \cdot u \cdot \xi^j \cdot a(i^*) + q \cdot v \cdot \xi^j \cdot x \pmod{pq}, \quad j \geqslant 0, \tag{7}$$

$$b(i^* + j \cdot S) \equiv p \cdot u \cdot \xi^j \cdot b(i^*) + q \cdot v \cdot \xi^j \cdot x \pmod{pq}, \quad j \geqslant 0. \tag{8}$$

Subtracting (8) from (7) leads to

$$a(i^* + j \cdot S) - b(i^* + j \cdot S) \equiv p \cdot u \cdot \xi^j \cdot a(i^*) - p \cdot u \cdot \xi^j \cdot b(i^*) \pmod{pq}, \quad j \geqslant 0.$$

By Property 2.1, this is equivalent to

$$\left[a(i^* + j \cdot S) - b(i^* + j \cdot S)\right]_{\bmod pq} = p \cdot \left[u \cdot \left(a(i^*) - b(i^*)\right) \cdot \xi^j\right]_{\bmod q}, \quad j \geqslant 0. \tag{9}$$

Suppose $a(i^*) \neq b(i^*) \pmod q$.

Since ξ is a primitive element modulo q and $\gcd(u,q)=1$, there exists an integer $J\geqslant 0$ for which

$$u\cdot\big(a(i^*)-b(i^*)\big)\cdot\xi^J\equiv 1 \pmod q. \tag{10}$$

Let $R=(q-1)/2$. Then by using $\xi^R\equiv -1 \pmod q$, it can be deduced from (10) that

$$u\cdot\big(a(i^*)-b(i^*)\big)\cdot\xi^{J+Rk}\equiv(-1)^k \pmod q,\quad k\geqslant 0. \tag{11}$$

Applying (9) with $j=J+R\cdot k$ and taking (11) into consideration, we have

$$\big[a(i^*+J\cdot S+R\cdot k\cdot S)-b(i^*+J\cdot S+R\cdot k\cdot S)\big]_{\bmod pq}=p\cdot\big[(-1)^k\big]_{\bmod q},\quad k\geqslant 0, \tag{12}$$

which immediately implies that either

$$a(i^*+J\cdot S+R\cdot k\cdot S)=b(i^*+J\cdot S+R\cdot k\cdot S)+p\cdot\big[(-1)^k\big]_{\bmod q},\quad k\geqslant 0, \tag{13}$$

or

$$a(i^*+J\cdot S+R\cdot k\cdot S)=b(i^*+J\cdot S+R\cdot k\cdot S)+p\cdot\big[(-1)^k\big]_{\bmod q}-pq,\quad k\geqslant 0. \tag{14}$$

But we have

$$a(i^*+J\cdot S+R\cdot k\cdot S)\equiv b(i^*+J\cdot S+R\cdot k\cdot S) \pmod 2,\quad k\geqslant 0,$$

by the assumption $\underline{a}\equiv\underline{b} \pmod 2$, and so only (13) holds if k is an odd number, i.e.,

$$a(i^*+J\cdot S+R\cdot k\cdot S)=b(i^*+J\cdot S+R\cdot k\cdot S)+p(q-1), \tag{15}$$

while only (14) holds if k is an even number, i.e.,

$$a(i^*+J\cdot S+R\cdot k\cdot S)=b(i^*+J\cdot S+R\cdot k\cdot S)+p-pq. \tag{16}$$

Thus, we can conclude that

$$a(i^*+J\cdot S+R\cdot k\cdot S)=b(i^*+J\cdot S+R\cdot k\cdot S)+(-1)^{k+1}\cdot p\cdot(q-1),\quad k\geqslant 0. \tag{17}$$

Case 1: $(q-1)$ is not divisible by $(p-1)$.
Let $k=2k'$ in (17). Then we have

$$a(i^*+J\cdot S+(q-1)\cdot k'\cdot S)=b(i^*+J\cdot S+(q-1)\cdot k'\cdot S)-p\cdot(q-1).$$

Note that $b(i^*+J\cdot S+(q-1)\cdot k'\cdot S)<pq$, and so

$$0<a(i^*+J\cdot S+(q-1)\cdot k'\cdot S)<p. \tag{18}$$

Since $p<q$, (18) implies that

$$a\big(i^* + J\cdot S + (q-1)\cdot k'\cdot S\big) = \big[a\big(i^* + J\cdot S + (q-1)\cdot k'\cdot S\big)\big]_{\bmod p} = \big[a\big(i^* + J\cdot S + (q-1)\cdot k'\cdot S\big)\big]_{\bmod q}. \tag{19}$$

Applying (7) with $j = J + (q-1)\cdot k'$ and using the identities given by (19), we get

$$a\big(i^* + J\cdot S + (q-1)\cdot k'\cdot S\big) = \big[x\cdot\xi^{(q-1)\cdot k'+J}\big]_{\bmod p} = \big[a\big(i^*\big)\cdot\xi^J\big]_{\bmod q}, \quad k' \geqslant 0. \tag{20}$$

Let $k' = 0$ and $k' = 1$, respectively. Then it can be observed from (20) that

$$x\cdot\xi^{(q-1)+J} \equiv x\cdot\xi^J \pmod p,$$

that is,

$$\xi^{q-1} \equiv 1 \pmod p.$$

Since ξ is a primitive element modulo p, $(q-1)$ must be divisible by $(p-1)$, a contradiction. Thus,

$$\big[a\big(i^*\big)\big]_{\bmod q} = \big[b\big(i^*\big)\big]_{\bmod q}.$$

Case 2: $(q-1)$ is divisible by $2(p-1)$.
First applying (7) with $j = J$ and $j = J + R$, respectively, we have

$$\begin{aligned} &a\big(i^* + J\cdot S\big) + a\big(i^* + J\cdot S + R\cdot S\big) \\ &\quad\equiv p\cdot u\cdot\xi^J\cdot a\big(i^*\big) + q\cdot v\cdot\xi^J\cdot x + p\cdot u\cdot\xi^{J+R}\cdot a\big(i^*\big) + q\cdot v\cdot\xi^{J+R}\cdot x \pmod{pq}. \end{aligned} \tag{21}$$

Note that $\xi^R \equiv -1 \pmod q$, and so (21) is equivalent to

$$a\big(i^* + J\cdot S\big) + a\big(i^* + J\cdot S + R\cdot S\big) \equiv q\cdot v\cdot\xi^J\cdot x\cdot\big(1+\xi^R\big) \pmod{pq},$$

i.e.,

$$\big[a\big(i^* + J\cdot S\big) + a\big(i^* + J\cdot S + R\cdot S\big)\big]_{\bmod pq} = q\cdot\big[v\cdot\xi^J\cdot x\cdot\big(1+\xi^R\big)\big]_{\bmod p}, \tag{22}$$

which implies that

$$a\big(i^* + J\cdot S\big) + a\big(i^* + J\cdot S + R\cdot S\big) \equiv 0 \pmod q. \tag{23}$$

Second, applying (17) with $k = 2k' + 1$, we have

$$a\big(i^* + J\cdot S + R\cdot(2k'+1)\cdot S\big) = b\big(i^* + J\cdot S + R\cdot(2k'+1)\cdot S\big) + p\cdot(q-1),$$

and so

$$p\cdot(q-1) < a\big(i^* + J\cdot S + R\cdot(2k'+1)\cdot S\big) < pq. \tag{24}$$

It follows from (18) and (24) that

$$pq - q < pq - p < a\big(i^* + J \cdot S\big) + a\big(i^* + J \cdot S + R \cdot S\big) < pq + p < pq + q. \tag{25}$$

Therefore (23) and (25) imply that

$$a\big(i^* + J \cdot S\big) + a\big(i^* + J \cdot S + R \cdot S\big) = pq. \tag{26}$$

Taking (26) into (22) we obtain

$$v \cdot \xi^J \cdot x \cdot \big(1 + \xi^R\big) \equiv 0 \pmod{p}.$$

Since $v \cdot \xi^J \cdot x \neq 0 \pmod{p}$, it shows that

$$\xi^R \equiv -1 \pmod{p},$$

a contradiction to the assumption that R is divisible by $(p-1)$. Thus

$$\big[a\big(i^*\big)\big]_{\bmod q} = \big[b\big(i^*\big)\big]_{\bmod q}. \qquad \square$$

Lemma 3.4. *Let $f(x)$ be a primitive polynomial of degree $n > 1$ over $Z/(pq)$ and $\underline{a}, \underline{b} \in G'(f(x), pq)$ with $\underline{a} \equiv \underline{b} \pmod 2$. If $p > q$ and the following two conditions are satisfied*:

(i) *there exist a positive integer S and a primitive element ξ in $Z/(pq)$ such that $x^S - \xi \equiv 0 \pmod{f(x), pq}$;*
(ii) *$(p-1)$ is not divisible by $(q-1)$ or $2(q-1)$ divides $(p-1)$,*

then

$$\big[a\big(i^*\big)\big]_{\bmod q} = \big[b\big(i^*\big)\big]_{\bmod q}$$

for any nonnegative integer i^* with $[a(i^*)]_{\bmod p} = [b(i^*)]_{\bmod p} \neq 0$.

Proof. Here the notations J, R and x are as described in Lemma 3.3.

From (18) and (24), we can conclude that

$$pq - p < pq - a\big(i^* + J \cdot S\big) < pq, \tag{27}$$

$$pq - p < a\big(i^* + J \cdot S + (2k+1) \cdot R \cdot S\big) < pq, \quad k \geqslant 0. \tag{28}$$

Let us denote $[a(i^* + J \cdot S)]_{\bmod q} = \delta$ and $p = m \cdot q + r$ with $1 \leqslant r \leqslant q-1$. Then

$$\big[pq - a\big(i^* + J \cdot S\big)\big]_{\bmod q} = q - \delta, \tag{29}$$

and also

$$\big[a\big(i^* + J \cdot S + (2k+1) \cdot R \cdot S\big)\big]_{\bmod q} = q - \delta, \quad k \geqslant 0, \tag{30}$$

because of

$$a\big(i^* + J \cdot S + (2k+1) \cdot R \cdot S\big) \equiv -a\big(i^* + J \cdot S\big) \pmod{q}, \quad k \geqslant 0.$$

Besides, it can be seen that there are at most $m+1$ different integers x between $pq-p+1$ and $pq-1$ for which $[x]_{\bmod q} = q-\delta$. Therefore, (27), (28), (29) and (30) imply that

$$a\big(i^* + J\cdot S + R\cdot S\big),\ a\big(i^* + J\cdot S + 3R\cdot S\big),\ \ldots,\ a\big(i^* + J\cdot S + (2m+1)\cdot R\cdot S\big)$$

and

$$pq - a\big(i^* + J\cdot S\big)$$

take on at most $m+1$ different values. We proceed the proof by showing this is impossible.

First, we claim

$$a\big(i^* + J\cdot S + R\cdot S\big),\ a\big(i^* + J\cdot S + 3R\cdot S\big),\ \ldots,\ a\big(i^* + J\cdot S + (2m+1)\cdot R\cdot S\big)$$

are distinct. Otherwise

$$a\big(i^* + J\cdot S + (2i+1)\cdot R\cdot S\big) = a\big(i^* + J\cdot S + (2j+1)\cdot R\cdot S\big) \tag{31}$$

for $0 \leqslant i < j \leqslant m$, then (31) implies that

$$x\cdot \xi^{J+(2i+1)R} \equiv x\cdot \xi^{J+(2j+1)R} \pmod p,$$

i.e.,

$$\xi^{2(j-i)R} \equiv 1 \pmod p. \tag{32}$$

On one hand, since $\xi \pmod p$ is a primitive element of $Z/(p)$, it follows from (32) that

$$(p-1) \mid (j-i)\cdot(q-1),$$

and so

$$(p-1) \leqslant (j-i)\cdot(q-1) \leqslant m\cdot(q-1). \tag{33}$$

On the other hand, we can deduce that

$$r+m \geqslant 2$$

from the assumption that p and q are different odd primes, and so

$$p-1 = m\cdot(q-1) + r + m - 1 > m\cdot(q-1),$$

which contradicts to (33). Thus

$$a\big(i^* + J\cdot S + R\cdot S\big),\ a\big(i^* + J\cdot S + 3R\cdot S\big),\ \ldots,\ a\big(i^* + J\cdot S + (2m+1)\cdot R\cdot S\big)$$

are distinct.

Second, we claim none of

$$a\big(i^* + J\cdot S + R\cdot S\big),\ a\big(i^* + J\cdot S + 3R\cdot S\big),\ \ldots,\ a\big(i^* + J\cdot S + (2m+1)\cdot R\cdot S\big)$$

is equal to $pq - a(i^* + J\cdot S)$. Otherwise, we have some integer k between 0 and m such that

$$a\big(i^* + J\cdot S + (2k+1)\cdot R\cdot S\big) = pq - a\big(i^* + J\cdot S\big),$$

from which we deduce

$$x\cdot\xi^{J+(2k+1)R} \equiv -x\cdot\xi^{J} \pmod{p},$$

i.e.,

$$\xi^{(2k+1)R} \equiv -1 \pmod{p}.$$

This implies that

$$(p-1)\mid(2k+1)\cdot(q-1) \quad \text{but} \quad 2(p-1)\nmid(2k+1)\cdot(q-1),$$

and so, considering $(2k+1)\cdot(q-1) \leqslant (2m+1)\cdot(q-1) < 3(p-1)$, we have

$$(2k+1)\cdot(q-1) = (p-1),$$

a contradiction to the assumption that $(p-1)$ is not divisible by $(q-1)$ or $2(q-1)$ divides $(p-1)$. Thus

$$a\big(i^* + J\cdot S + R\cdot S\big),\ a\big(i^* + J\cdot S + 3R\cdot S\big),\ \ldots,\ a\big(i^* + J\cdot S + (2m+1)\cdot R\cdot S\big)$$

and

$$pq - a\big(i^* + J\cdot S\big)$$

are distinct. The lemma is proved. □

Combining the results of Lemmas 3.2, 3.3 and 3.4 we arrive at the following conclusion.

Corollary 3.1. *Let $f(x)$ be a primitive polynomial of degree $n > 1$ over $Z/(pq)$ and $\underline{a}, \underline{b} \in G'(f(x), pq)$ with $\underline{a} \equiv \underline{b} \pmod 2$. If $p < q$ and the following two conditions are satisfied:*

(i) *there exist a positive integer S and a primitive element ξ in $Z/(pq)$ such that $x^S - \xi \equiv 0 \pmod{f(x), pq}$;*
(ii) *$(q-1)$ is not divisible by $(p-1)$ or $2(p-1)$ divides $(q-1)$,*

then $[a(i^*)]_{\bmod p} = [b(i^*)]_{\bmod p}$ if and only if $[a(i^*)]_{\bmod q} = [b(i^*)]_{\bmod q}$ for any integer $i^* \geqslant 0$.

Remark 3.1. It can be seen that the second condition in Corollary 3.1 is equivalent to say $(q-1) \neq (2k+1)\cdot(p-1)$ for any integer $k \geqslant 0$.

With above preparations, we are ready to prove the first main result of this section.

Theorem 1. *Let $f(x)$ be a primitive polynomial of degree $n > 1$ over $Z/(pq)$, and $\underline{a}, \underline{b} \in G'(f(x), pq)$. If $p < q$ and the following two conditions are satisfied*:

(i) *there exist a positive integer S and a primitive element ξ in $Z/(pq)$ such that $x^S - \xi \equiv 0 \pmod{f(x), pq}$;*
(ii) *$(q-1) \neq (2k+1)\cdot(p-1)$ for arbitrary integer k,*

then $\underline{a} \equiv \underline{b} \pmod 2$ if and only if $\underline{a} = \underline{b}$.

Proof. The sufficient condition is trivial. In the following we will discuss the necessary condition. From Corollary 3.1, we know that

$$a(i) \equiv b(i) \pmod p \quad \text{if and only if} \quad a(i) \equiv b(i) \pmod q, \tag{34}$$

for any integer $i \geqslant 0$. Therefore, if $\underline{a} \equiv \underline{b} \pmod p$ or $\underline{a} \equiv \underline{b} \pmod q$, then the theorem is proved.

Suppose $\underline{a} \neq \underline{b} \pmod p$ and $\underline{a} \neq \underline{b} \pmod q$ in the following.

Because $\underline{a} - \underline{b} \pmod p$ and $\underline{a} - \underline{b} \pmod q$ are m-sequences of degree n over $Z/(p)$ and $Z/(q)$, respectively, we have

$$N_p(\underline{a} - \underline{b}, 0) = p^{n-1} - 1, \tag{35}$$

$$N_q(\underline{a} - \underline{b}, 0) = q^{n-1} - 1. \tag{36}$$

By considering successive $\operatorname{lcm}(p^n - 1, q^n - 1)$ elements of $\underline{a}$ and $\underline{b}$, (34) implies that

$$\frac{\operatorname{lcm}(p^n-1, q^n-1)}{p^n-1} N_p(\underline{a} - \underline{b}, 0) = \frac{\operatorname{lcm}(p^n-1, q^n-1)}{q^n-1} N_q(\underline{a} - \underline{b}, 0). \tag{37}$$

Then (35), (36) and (37) lead to

$$\frac{p^{n-1}-1}{p^n-1} = \frac{q^{n-1}-1}{q^n-1}. \tag{38}$$

This is impossible since $p < q$ and $n > 1$. Thus the theorem is proved. □

3.2. About the existence of S

It can be seen that the assumption that there exist a positive integer S and a primitive element ξ in $Z/(pq)$ such that $x^S - \xi \equiv 0 \bmod (f(x), pq)$ plays a key role in the proofs of last subsection. Then it may be asked how about the existence of such S. This subsection is just devoted to the discussion of that.

First of all, let us see a standard result about primitive polynomials over finite fields, see [21].

Proposition 3.1. *(See [21].) Let p be an odd prime and $f(x)$ be a primitive polynomial of degree $n > 1$ over $Z/(p)$. Then there exists a primitive element ξ in $Z/(p)$ such that*

$$x^{\frac{p^n-1}{p-1}} \equiv \xi \pmod{f(x), p}.$$

Lemma 3.5. *Let p_1 and p_2 be two different odd primes, $f(x)$ be a primitive polynomial of degree n over $Z/(p_1p_2)$ and S be a positive integer. If*

$$\gcd\left(S, p_i^n - 1\right) = \frac{p_i^n - 1}{p_i - 1}, \quad i = 1, 2, \tag{39}$$

then there exists a primitive element ξ in $Z/(pq)$ such that

$$x^S - \xi \equiv 0 \pmod{f(x), p_1 p_2}.$$

Proof. Since

$$\gcd(S, p_i^n - 1) = \frac{p_i^n - 1}{p_i - 1}, \quad i = 1, 2,$$

by Proposition 3.1 we know there exists a primitive element ξ_i in $Z/(p_i)$ such that

$$x^S \equiv \xi_i \pmod{f(x), p_i} \tag{40}$$

for $i = 1, 2$. Then it follows from Chinese Remainder Theorem that there exists a primitive element ξ in $Z/(p_1 p_2)$ for which

$$\xi \equiv \xi_i \pmod{p_i}, \quad i = 1, 2. \tag{41}$$

Therefore, (40) and (41) imply that $x^S \equiv \xi \pmod{f(x), p_1 p_2}$. This completes the proof. □

Remark 3.2. In fact, the condition in Lemma 3.5 is not only a sufficient condition but also a necessary condition.

It is clear that if S satisfies (39) of Lemma 3.5, then S is divisible by $\operatorname{lcm}(\frac{p_1^n-1}{p_1-1}, \frac{p_2^n-1}{p_2-1})$ and $\operatorname{lcm}(\frac{p_1^n-1}{p_1-1}, \frac{p_2^n-1}{p_2-1})$ also satisfies (39). Note that for any pair of (p_1, p_2), we only need to find one such "S," and so it suffices to consider the case $S = \operatorname{lcm}(\frac{p_1^n-1}{p_1-1}, \frac{p_2^n-1}{p_2-1})$. Accordingly, the following lemma further presents a sufficient condition on $\operatorname{lcm}(\frac{p_1^n-1}{p_1-1}, \frac{p_2^n-1}{p_2-1})$.

Lemma 3.6. *Let p_1 and p_2 be two different odd primes, $f(x)$ be a primitive polynomial of degree n over $Z/(p_1 p_2)$ and*

$$S = \operatorname{lcm}\left(\frac{p_1^n - 1}{p_1 - 1}, \frac{p_2^n - 1}{p_2 - 1}\right).$$

If

$$\gcd\left(p_1 - 1, \frac{p_2^n - 1}{p_2 - 1}\right) = \gcd\left(p_2 - 1, \frac{p_1^n - 1}{p_1 - 1}\right) = 1,$$

then there exists a primitive element ξ in $Z/(p_1 p_2)$ such that

$$x^S - \xi \equiv 0 \pmod{f(x), p_1 p_2}.$$

Proof. From Lemma 3.5, we know it suffices to show

$$\gcd(S, p_i^n - 1) = \frac{p_i^n - 1}{p_i - 1}, \quad i = 1, 2. \tag{42}$$

In the following we only consider the case of $i = 1$, and as for the other case, the proof is an analogue. Note that

$$S = \operatorname{lcm}\left(\frac{p_1^n - 1}{p_1 - 1}, \frac{p_2^n - 1}{p_2 - 1}\right) = \frac{\frac{p_1^n-1}{p_1-1} \cdot \frac{p_2^n-1}{p_2-1}}{\gcd(\frac{p_1^n-1}{p_1-1}, \frac{p_2^n-1}{p_2-1})},$$

which is divisible by $(p_1^n - 1)/(p_1 - 1)$, and so (42) is equivalent to

$$\gcd\left(\frac{\frac{p_2^n-1}{p_2-1}}{\gcd(\frac{p_1^n-1}{p_1-1}, \frac{p_2^n-1}{p_2-1})}, p_1 - 1\right) = 1.$$

This is an immediate consequence of the assumption $\gcd(p_1 - 1, \frac{p_2^n-1}{p_2-1}) = 1$. Thus the lemma is proved. □

Remark 3.3. Although Lemma 3.6 assumes a stronger condition than Lemma 3.5, the condition of Lemma 3.6 is easier to verify.

3.3. Primitive polynomials of degree 1

Theorem 2. *Let p and q be two different odd primes with $\gcd(p - 1, q - 1) = 2$, and let $f(x) = x - \xi$, where ξ is a primitive element in $Z/(pq)$. If*

$$\frac{p-1}{\operatorname{ord}_p(2)} \equiv \frac{q-1}{\operatorname{ord}_q(2)} \pmod 2,$$

then $\underline{a} \equiv \underline{b} \pmod 2$ if and only if $\underline{a} = \underline{b}$ for $\underline{a}, \underline{b} \in G'(f(x), pq)$.

Proof. It suffices to prove the necessary condition. Note that $\underline{a}$ and $\underline{b}$ can be represented as

$$a(i) \equiv \xi^i \cdot a(0) \pmod{pq}, \quad i \geqslant 0,$$
$$b(i) \equiv \xi^i \cdot b(0) \pmod{pq}, \quad i \geqslant 0.$$

It follows from $\underline{a} \equiv \underline{b} \pmod 2$ that

$$\left[\xi^i \cdot a(0)\right]_{\bmod pq} \equiv \left[\xi^i \cdot b(0)\right]_{\bmod pq} \pmod 2, \quad i \geqslant 0. \tag{43}$$

Suppose $\xi \equiv 2^{-1} \pmod{pq}$. Then by (43) and Lemma 2.2, we can obtain that

$$-\frac{a(0)}{pq} = \sum_{i=0}^{\infty} \left[a(i)\right]_{\bmod 2} \cdot 2^i = \sum_{i=0}^{\infty} \left[b(i)\right]_{\bmod 2} \cdot 2^i = -\frac{b(0)}{pq}.$$

Hence $a(0) = b(0)$.

Suppose $\xi \neq 2^{-1} \pmod{pq}$. Firstly, we prove that there exists a positive integer h such that $\xi^h \equiv 2^{-1} \pmod{pq}$.

Let $c = \operatorname{ord}_p(2)$ and $d = \operatorname{ord}_q(2)$. By the basic theory of finite fields, we know there exist a primitive element η_p in $Z/(p)$ and a primitive element η_q in $Z/(q)$ such that

$$[2]_{\bmod p} = \left[\eta_p^{(p-1)/c}\right]_{\bmod p},$$
$$[2]_{\bmod q} = \left[\eta_q^{(q-1)/d}\right]_{\bmod q}.$$

It follows from Chinese Remainder Theorem that there exists a primitive element η in $Z/(pq)$ such that

$$\eta \equiv \eta_p \pmod{p} \quad \text{and} \quad \eta \equiv \eta_q \pmod{q},$$

which imply that

$$[2]_{\bmod p} = \left[\eta^{(p-1)/c}\right]_{\bmod p},$$
$$[2]_{\bmod q} = \left[\eta^{(q-1)/d}\right]_{\bmod q}.$$

Since ξ is a primitive element in $Z/(pq)$, there must exist positive integers l_1 and l_2 such that $\gcd(l_1, p-1) = 1$, $\gcd(l_2, q-1) = 1$ and

$$[2]_{\bmod p} = \left[\xi^{l_1\cdot(p-1)/c}\right]_{\bmod p},$$
$$[2]_{\bmod q} = \left[\xi^{l_2\cdot(q-1)/d}\right]_{\bmod q}.$$

Note that l_1 and l_2 are two odd integers, it follows from

$$(p-1)/\operatorname{ord}_p(2) \equiv (q-1)/\operatorname{ord}_q(2) \pmod{2}$$

that

$$\frac{(p-1)\cdot l_1}{c} \equiv \frac{(q-1)\cdot l_2}{d} \pmod{2}.$$

Since $\gcd(p-1, q-1) = 2$, we can deduce from Euclidean algorithm that there exist two integer k_1 and k_2 such that

$$k_1\cdot(p-1) - k_2\cdot(q-1) = \frac{(q-1)\cdot l_2}{d} - \frac{(p-1)\cdot l_1}{c}.$$

Set

$$t = \frac{(p-1)\cdot l_1}{c} + k_1\cdot(p-1) = \frac{(q-1)\cdot l_2}{d} + k_2\cdot(q-1).$$

Then

$$\xi^t \equiv \xi^{l_1\cdot(p-1)/c + k_1\cdot(p-1)} \equiv \xi^{l_1\cdot(p-1)/c} \equiv 2 \pmod{p},$$
$$\xi^t \equiv \xi^{l_2\cdot(q-1)/d + k_2\cdot(q-1)} \equiv \xi^{l_2\cdot(q-1)/d} \equiv 2 \pmod{q},$$

i.e.,

$$\xi^t \equiv 2 \pmod{pq},$$

which implies that $\xi^{\varphi(pq)-t} \equiv 2^{-1} \pmod{pq}$, where $\varphi(pq) = (p-1)(q-1)$. Thus

$$h = \varphi(pq) - t$$

is the desired integer.

Secondly, we consider the h-fold decimation of $\underline{a}$ and $\underline{b}$. For arbitrary integer $i \geqslant 0$, we have

$$a(h \cdot i) \equiv \left(\xi^h\right)^i \cdot a(0) \equiv 2^{-i} \cdot a(0) \pmod{pq},$$
$$b(h \cdot i) \equiv \left(\xi^h\right)^i \cdot b(0) \equiv 2^{-i} \cdot b(0) \pmod{pq}.$$

From $\underline{a} \equiv \underline{b} \pmod 2$, we have

$$a(h \cdot i) \equiv b(h \cdot i) \pmod 2,$$

i.e.,

$$\left[2^{-i} \cdot a(0)\right]_{\bmod pq} \equiv \left[2^{-i} \cdot b(0)\right]_{\bmod pq} \pmod 2.$$

By Lemma 2.2, we get

$$-\frac{a(0)}{pq} = \sum_{i=0}^{\infty} \left[a(h \cdot i)\right]_{\bmod 2} \cdot 2^i = \sum_{i=0}^{\infty} \left[b(h \cdot i)\right]_{\bmod 2} \cdot 2^i = -\frac{b(0)}{pq}.$$

Thus $a(0) = b(0)$. □

Remark 3.4. Condition $(p-1)/\operatorname{ord}_p(2) \equiv (q-1)/\operatorname{ord}_q(2) \pmod 2$ in Theorem 2 is equivalent to

$$2^{(p-1)/2} \equiv 1 \pmod p \quad \text{if and only if} \quad 2^{(q-1)/2} \equiv 1 \pmod q.$$

3.4. On special cases

Note that Theorem 1 is not valid for the case of $Z/(3p)$ with $p \equiv 3 \pmod 4$. However, we can get the following result about the case by Theorem 2.

Corollary 3.2. *Let p be an odd prime with $p \equiv 3 \pmod 4$ and $f(x)$ be a primitive polynomial of degree $n > 1$ over $Z/(3p)$, $\underline{a}, \underline{b} \in G'(f(x), 3p)$. If*

(i) *there exist a positive integer S and a primitive element ξ in $Z/(3p)$ such that $x^S - \xi \equiv 0 \pmod{f(x), 3p}$;*
(ii) $2^{(p-1)/2} \equiv -1 \pmod p$,

then $\underline{a} \equiv \underline{b} \pmod 2$ if and only if $\underline{a} = \underline{b}$.

Proof. It suffices to prove the necessary condition. Suppose $\underline{a} \neq \underline{b}$, without loss of generality, we assume $a(0) \neq b(0)$. From (1) and condition (i) we have

$$a(j \cdot S) \equiv \xi^j \cdot a(0) \pmod{3p}, \quad j \geqslant 0,$$
$$b(j \cdot S) \equiv \xi^j \cdot b(0) \pmod{3p}, \quad j \geqslant 0.$$

Since $\underline{a} \equiv \underline{b} \pmod 2$, then

$$\left[\xi^j \cdot a(0)\right]_{\bmod 3p} \equiv \left[\xi^j \cdot b(0)\right]_{\bmod 3p} \pmod 2, \quad j \geqslant 0. \tag{44}$$

Note that both $\{[\xi^j \cdot a(0)]_{\bmod 3p}\}_{j\geqslant 0}$ and $\{[\xi^j \cdot b(0)]_{\bmod 3p}\}_{j\geqslant 0}$ can be considered as sequences generated by $x-\xi$ over $Z/(3p)$. By (44) and condition (ii), we can conclude from Theorem 2 that

$$a(0) = b(0).$$

This contradicts to the assumption of $a(0) \neq b(0)$. Thus $\underline{a} = \underline{b}$. □

Using the assumption $\gcd(p-1, q-1) = 2$ in Theorem 2, we can also get a result on primitive polynomials of odd degrees.

Corollary 3.3. *Let p and q be two different odd primes with $3 < p < q$ and $f(x)$ be a primitive polynomial of an odd degree n over $Z/(pq)$. If*

$$\gcd\big(p^n - 1, q-1\big) = \gcd\big(q^n - 1, p-1\big) = 2,$$

then $\underline{a} \equiv \underline{b} \pmod 2$ if and only if $\underline{a} = \underline{b}$ for $a, b \in G'(f(x), pq)$.

Proof. It suffices to prove the necessary condition. Since n is an odd integer, we have

$$\big(q^n - 1\big)/(q-1) \equiv \big(p^n - 1\big)/(p-1) \equiv 1 \pmod 2.$$

Thus it can be deduced from the assumption of the corollary that

$$\gcd(p-1, q-1) = 2$$

and

$$\gcd\left(p-1, \frac{q^n-1}{q-1}\right) = \gcd\left(q-1, \frac{p^n-1}{p-1}\right) = 1,$$

and also $(q-1)$ is not divisible by $(p-1)$. Then the corollary follows from Theorem 1 and Lemma 3.6. □

4. Conclusions

Let p and q be two different prime numbers, and let $f(x)$ be a primitive polynomial over $Z/(pq)$ such that $f(x) \pmod p$ and $f(x) \pmod q$ are primitive over $Z/(p)$ and $Z/(q)$, respectively. Given two maximal length sequences $\underline{a}$ and $\underline{b}$ both of which are generated by $f(x)$ over $Z/(pq)$, it is shown in this paper that $\underline{a} \pmod 2$ and $\underline{b} \pmod 2$ are distinct if p, q and $\deg f(x)$ satisfy certain conditions. For $2 \leqslant \deg f(x) \leqslant 31$ and $p, q < 1000$, experimental evidence shows that the proportion of $(\deg f(x), p, q)$ satisfying the assumption of Theorem 1 is about 48.76%. Furthermore, for this case, it seems that such distinctness property always holds. But for the case of $\deg f(x) = 1$, there indeed exist some counterexamples.

Acknowledgments

The authors are grateful to the reviewers for their helpful comments and suggestions.

References

[1] M.Q. Huang, Z.D. Dai, Projective maps of linear recurring sequences with maximal p-adic periods, Fibonacci Quart. 30 (2) (1992) 139–143.
[2] A.S. Kuzmin, A.A. Nechaev, Linear recurring sequences over Galois ring, Russian Math. Surveys 48 (1993) 171–172.
[3] M.Q. Huang, Analysis and cryptologic evaluation of primitive sequences over an integer residue ring, PhD dissertation, Graduate School of USTC, Academia Sinica, Beijing, China, 1988.
[4] W.F. Qi, J.H. Yang, J.J. Zhou, ML-sequences over rings $Z/(2^e)$, in: Advances in Cryptology ASIACRYPT'98, in: Lecture Notes in Comput. Sci., vol. 1514, Springer-Verlag, Berlin, 1998, pp. 315–325.
[5] W.F. Qi, Compressing maps of primitive sequences over $Z/(2^e)$ and analysis of their derivative sequences, PhD dissertation, Zhengzhou Inform. Eng. Univ., Zhengzhou, China, 1997.
[6] W.F. Qi, X.Y. Zhu, Compressing mappings on primitive sequences over $Z/(2^e)$ and its Galois extension, Finite Fields Appl. 8 (4) (2002) 570–588.
[7] X.Y. Zhu, W.F. Qi, Compression mappings on primitive sequences over $Z/(p^e)$, IEEE Trans. Inform. Theory 50 (10) (2004) 2442–2448.
[8] X.Y. Zhu, W.F. Qi, Further result of compressing maps on primitive sequences modulo odd prime powers, IEEE Trans. Inform. Theory 53 (8) (2007) 2985–2990.
[9] T. Tian, W.F. Qi, Injectivity of compressing maps on primitive sequences over $Z/(p^e)$, IEEE Trans. Inform. Theory 53 (8) (2007) 2966–2970.
[10] X.Y. Zhu, W.F. Qi, Uniqueness of the distribution of zeroes of primitive level sequences over $Z/(p^e)$, Finite Fields Appl. 11 (1) (2005) 30–44.
[11] X.Y. Zhu, W.F. Qi, Uniqueness of the distribution of zeroes of primitive level sequences over $Z/(p^e)$ (II), Finite Fields Appl. 13 (2) (2007) 230–248.
[12] A. Klapper, M. Goresky, 2-Adic shift registers, in: Proc. of 1993 Cambridge Security Workshop, Fast Software Encryption, in: Lecture Notes in Comput. Sci., vol. 809, Springer-Verlag, New York, 1993, pp. 174–178.
[13] M. Goresky, A. Klapper, Arithmetic crosscorrelations of feedback with carry shift register sequences, IEEE Trans. Inform. Theory 43 (4) (1997) 1342–1345.
[14] M. Goresky, A. Klapper, Fourier transforms and the 2-adic span of periodic binary sequences, IEEE Trans. Inform. Theory 46 (2000) 687–691.
[15] C. Seo, S. Lee, Y. Sung, K. Han, S. Kim, A lower bound on the linear span of an FCSR, IEEE Trans. Inform. Theory 46 (2) (2000) 691–693.
[16] W.F. Qi, H. Xu, Partial period distribution of FCSR sequences, IEEE Trans. Inform. Theory 49 (3) (2003) 761–765.
[17] H. Xu, W.F. Qi, Further results on the distinctness of decimations of l-sequences, IEEE Trans. Inform. Theory 52 (8) (2006) 3831–3836.
[18] H. Xu, W.F. Qi, Autocorrelations of maximum period FCSR sequences, SIAM J. Discrete Math. 20 (3) (2006) 568–577.
[19] A. Klapper, M. Goresky, Feedback shift registers, 2-adic span, and combiners with memory, J. Cryptology 10 (2) (1997) 111–147.
[20] X.Y. Zhu, W.F. Qi, On the distinctness of modular reductions of maximal length sequences modulo odd prime powers, Math. Comp. 77 (2008) 1623–1637.
[21] R. Lidl, H. Niedereiter, Finite Field, Addison–Wesley, Canada, 1983.